



Cyber-Safety for Mobile Workers



Mobile working is when an employee works from a location other than the office. They could be at home, a café, or on a train.

It is important to stay secure even when you aren't at the office. By following some simple practices, you can go a long way to protecting yourself and any sensitive information you work with.

Use a secure wireless network

- If you are using a laptop, ensure that you are connected to a trusted and secure wireless network.
- If you must use a public network then avoid performing sensitive or business critical activities and if possible, connect with a Virtual Private Network (VPN).
- The most effective steps you can take to secure your home wireless network is to:
 - change the default administrator password on your wireless router(s),
 - enable WPA2 encryption, and
 - use a strong password for your wireless network.

Refer to your router manual for assistance.

Be aware of Phishing and Social Engineering

Cyber criminals register and use related website names to steal usernames and passwords, commit fraud, and launch malware related attacks. Mobile devices are also vulnerable to text and phone scams. Be security smart by:

- Avoiding opening emails from unknown sources; only clicking on links or open attachments from known sources after hovering over the link for verification,
- Recognizing and deleting spam messages purporting to be from official sources,
- Never providing any personal information including user names, password or account numbers, and
- Confirming email legitimacy of the sender by contacting the source by another means such as telephone or separate email after verifying the information with another source.





- **Protect the information in your care**
Never post pictures of your work space online.
- **Lock your mobile device when not in use**
Locking your device screen with a password ensures others cannot access the information on your device.
- **Store any documents securely**
If you do not choose to bring them back to the workplace, dispose of paper documents by using a shredder or secure disposal bin.
- **Protect against shoulder surfing**
Working in a shared environment requires that you do not inadvertently display confidential information to people viewing your screen. Consider using a privacy filter which blocks the view of your screen from people sitting nearby.
- **Lock your screen before you leave**
Ensure you lock your screen (Ctrl+Alt+Delete or the Windows key+ L) or log out before leaving your computer. Shutdown your device when you will be gone for an extended period.
- **Keep your device secured/tethered**
If for some reason you need to leave your device alone for a few minutes, and the option exists, use a locking cable to tether the device to something heavy and secure.

- **Know who (or what) is listening**
Be aware of personal assistants (ie. Alexa, Google Home) or mobile devices that may be listening to your confidential discussion. Turn them off or remove them from the room.
- **Make phone or video calls in private**
If you are unable to secure a private room, be aware of your surroundings and what other conference members will be able to see in the background.
- **Keep your device updated**
Ensure that you receive the latest updates to your government issued work device through the *Software Centre* and keep your personal devices OS and applications up-to-date through (and ONLY through) the vendors' update/upgrade pages.
- **Maintain a clean work area**
If you are leaving your temporary workplace, ensure that you clean the area of any work documents, especially confidential ones
- **Immediately report a lost or stolen device**
If the device was accessed by an unauthorized person or if it is lost or stolen, report it to your employer and your local police department.
 - Government Employees must contact 250 387-7000 or toll-free at 1-866-660-0811, Select Option 4

Resources:

Microsoft Security
Get Safe Online
The Security Company
Canadian Centre for Cyber Security Information Website

<https://www.microsoft.com>
<https://getsafeonline.org>
<https://www.thesecuritycompany.com>
<https://www.cyber.gc.ca/en/staying-cyber-safe-while-teleworking>

